

## Re: [Full-Disclosure] east coast powergrid / SCADA [OT?]

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-08/1058.html>

---

**From:** Stephen Clowater ([steve\\_at\\_stevesworld.hopto.org](mailto:steve_at_stevesworld.hopto.org))

**Date:** 08/17/03

To: <[cta@hcsin.net](mailto:cta@hcsin.net)>, <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>

Date: Sat, 16 Aug 2003 20:37:40 -0300

----- Original Message -----

From: "Bernie, CTA" <[cta@hcsin.net](mailto:cta@hcsin.net)>

To: <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>

Sent: Saturday, August 16, 2003 2:25 PM

Subject: Re: [Full-Disclosure] east coast powergrid / SCADA [OT?]

> On 16 Aug 2003 at 5:36, Stephen Clowater wrote:  
> > Its highly unlikely that msblast had anything to do with the  
> > power outage. For one, the internal rpc network that is used to  
> > monitor actual power spikes, and to move current from one circuit  
> > to the next in a grid is a closed network. And in the areas were  
> > it cant be closed (between major utilities) it is tunned via a  
> > VPN. Yes it runs a bit of NT4 and a bit of Windows 2000, In the  
> > next few years there has been a plan proposed to make freeBSD a  
> > standard.  
> >  
> > MSblast did not cause this, there have been warnings for the last  
> > 10 years that the grid was overloaded in the particular ring were  
> > the overload started. For years people have been warning that if  
> > a major transmittion line went during a high demand period of  
> > time, then you could be looking at a surge larger than can be  
> > midigated coming out of that ring. And then when it happens  
> > people come up with this theory that its msblast? Please, if that  
> > were the case, why have none of hte other billons of windows  
> > vunerabilities ever affected the grid? more specifically, why  
> > havent any of the thousands of rpc vunerabilites ever effected  
> > the grid?  
> >  
> > And sure enough, this morning on CNN, officals said they have a  
> > working theory that a major transmission line inside the ring  
> > went, wich created a back wave in the grid until it finaly came  
> > around in the form of a hudge surge. Niagra somehow saw this  
> > coming and shut down all generators in time to stay on the grid,  
> > and as the failure expanded more failsafes kicked in to contain  
> > it.

Re: [Full-Disclosure] east coast powergrid / SCADA [OT?]

> >  
> > *This is far from a complete explanation. But it fits the*  
> > *available facts, it fits the timetable of what happened, and it*  
> > *makes logical sense in relation to the recent history of the*  
> > *power grid.*  
> >  
> > *Now can we give msblast a rest? :)*  
> >  
>  
> *No, not yet...*  
>  
> *First of all, it is unrealistic to assume that the power plants,*  
> *distribution nodes and sub stations are still equipped with 1965*  
> *technology. Have you ever visited any of these facilities? I*  
> *have.*

That's not what I said, what I said was the warnings that had been coming for the last 10 years that this could happen, the situation in California a few years ago and the grid failures on the west coast in 1996 can also attest to this. And yes I have visited these facilities, and done work in them.

>  
> *Back in the 60s the primary feeder topology concerning supply*  
> *and demand, onto and from, the grid were simplex, and the fault*  
> *safeguards transient response capability was poor and typically*  
> *lacked the ability to quickly switch/isolate or arrest a power*  
> *surge to avoid or divert fault currents/voltages from*  
> *propagating throughout the Grid. That is to say, most of the*  
> *instrumentation was analog as were the safeguards, there were*  
> *mechanical switchgear and humans pushing buttons.*  
>  
> *Today the primary feeders topology consists of duplicated paths*  
> *of supply from a single power source, and are mostly controlled*  
> *by sophisticated computers with active fault isolation*  
> *mechanisms. In addition, there are many active and passive*  
> *safety components, transient fault, overload, ground-fault,*  
> *sensing current as well as voltage at all entry-points onto the*  
> *grid. Sophisticated active lightning arresters (valve-type and*  
> *expulsion-type, etc), ranging from station class > 1000kVA,*  
> *intermediate-class <1000kVA to distribution-class < 46kV.*  
>

It has been confirmed that this was caused by lightning. And the sophisticated computers used to distribute power inside plants, they are used to sense the demand and adjust the generators accordingly, and to act as breaker systems in the event the plant is cut from the grid. However, the issue here is not these systems, it has already been confirmed that whatever happened happened while power was in transit. Presumably, at this point, in the loop, the only computer systems in substations and on the wires themselves are proprietary systems that are loaded into banks of 1024K block chips and then integrated into the system. These systems don't even

know about tcp, let alone the RPC.

- > *Lightning voltage "potential" has been estimated to be between*
- > *100 million and 1 billion volts. However, protection engineers*
- > *are mostly concerned with the potential that appears on the line*
- > *conductors "transmission lines". This potential is obtained by*
- > *multiplying the current by the surge impedance Z of the*
- > *conductor. The potential which can appear upon any apparatus*
- > *connected to the Grid / Towers is limited only by either*
- > *protective measures or flashover of insulating components. Most*
- > *towers have magnetic link mechanisms to read currents in the*
- > *tower legs. Historical data shows that increase in current*
- > *amplitudes resulting from a direct lightning stroke have been*
- > *recorded in excess of 10,000 Amps. However, only 10% of the*
- > *tower currents are in excesses of 32,000 Amps.*
- >

The tower where the initial failure in the cascade occurred was carrying 31,500 amps.

Moreover, lightning has been ruled out as a possible cause. So lightning protective measures really had no impact on any aspects of this outage.

- > *With that being said, the transient response, i.e. the speed at*
- > *which a surge could propagate is directly related to the*
- > *conductors transient impedance. Typically, this transient*
- > *(surge) impedance lies between 400 and 500 ohms for transmission*
- > *lines. Consequently, assuming a straight path with no*
- > *interdiction the typical velocity of propagation for*
- > *transmission lines is 1000 ft / micro sec, 1 Mile / 5.28 micro*
- > *sec, or 100 miles in about 528 micro sec.*
- >
- > *Now lets assume that the distance between the strike zone and*
- > *the next entry-point onto the Grid is 100 Miles. The safeguards,*
- > *which are automated, would in theory have more than 500 micro*
- > *seconds to respond. Considering the surge valves and other*
- > *protective apparatus along the path, I find it implausible to*
- > *accept that all of the switchgear and surge arresters failed to*
- > *react within the 500us timeframe in order to isolate, divert and*
- > *arrest the surge, and place alternative power sources on the*
- > *Grid.*

This isn't really the issue. The issue is that the entire grid is operating at close to 90% of its capacity, when a failure occurs, and the current is diverted, it's being diverted to another overloaded line, which pushes that overloaded line to above its capacity, which then diverts it to another line, which pushes that line over its capacity, etc etc. Which is consistent with the warnings that have been received since the early 80's that during peak demand times (the time of day and the time of year were both at peak for demand with this occurred) could trigger a domino effect over the grid.

- >
- > *Sorry, but the lightning bolt theory alone is far fetched even*
- > *if we apply chaos theory, or completely dispense with the*
- > *statistical principle of goodness-of-fit.*

The lightning bolt theory has already been ruled out. And was ruled out before the first night of outage was over. The working theory that the initial data out of the investigation is that it was a transmission failure inside the loop that caused current to begin moving irregularly and ultimately ended in a massive surge coming from the loop and traveling back down the grid. Monitoring stations at Niagra saw what is now believed to be this and initiated emergency shut downs on their generators.

- >
- > *I still feel that there was human intervention to disrupt or*
- > *otherwise circumvent the automatic safeguards, in response to an*
- > *anomaly (i.e. MSBlaster). Or there was a lightning strike, BUT*
- > *the protection measure failed to properly engage due to the*
- > *MSBlaster, or again human intervention due to vulnerabilities in*
- > *the protection monitoring and control systems. That is, maybe*
- > *the automated protection systems were off line and being*
- > *upgraded due to the threat of MSBlaster or otherwise.*
- > *Furthermore, maybe a power surge did occur due to a lightning*
- > *bolt or demand power surge, but the human could not respond in*
- > *500us. After all, how many Jackie Chans are power plant*
- > *operators.*
- >
- > *Please feel free to shoot this theory to pieces.*

This is precisely what has been warned by people in the energy community for years. In fact, the former head of the dept of energy on CNN thurs Night said "america is a first world nation with a third world power grid". President Bush was quoted the next day as calling the power grid "antiquated".

The problem is that the grid that is around today was initially constructed in a time where power plants served a local area. Now power plants ship power via the grid over hundreds of miles. Over a grid that was not designed to be continually distributing power. It was designed to pick up the slack. Not be the principle transmitter of the power. The power grid is old, the plants on it are not. The available evidence at this point, and the logical course at this point would be that the initial report out of the loop that a major transmission line failure (which was confirmed by the responsible utility) of a line carrying a current of approx 31,500 amps, triggered a massive displacement and subsequent overload inside the loop, which then spread throughout the system in a matter of seconds. After these few seconds, safety measures caught up to the surge and was able to mitigate it and eventually stop the outage.

- >
- > -

Full-Disclosure: Re: [Full-Disclosure] east coast powergrid / SCADA [OT?]

> \*\*\*\*\*  
> *Bernie*  
> *Chief Technology Architect*  
> *Chief Security Officer*  
> *cta@hcsin.net*  
> *Euclidean Systems, Inc.*  
> \*\*\*\*\*  
> // *"There is no expedient to which a man will not go*  
> // *to avoid the pure labor of honest thinking."*  
> // *Honest thought, the real business capital.*  
> // *Observe> Think> Plan> Think> Do> Think>*  
> \*\*\*\*\*  
>  
>  
>  
> \_\_\_\_\_  
> *Full-Disclosure – We believe in it.*  
> *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*  
>

\_\_\_\_\_  
Full-Disclosure – We believe in it.  
Charter: <http://lists.netsys.com/full-disclosure-charter.html>